(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: 11068730 A

(43) Date of publication of application: 09 . 03 . 99

(51) Int. Cl H04L 9/08
H04L 9/10
H04L 12/46
H04L 12/28
H04L 12/66

(21) Application number: 09220478

(22) Date of filing: 15 . 08 . 97

(71) Applicant: NEC COMMUN SYST LTD

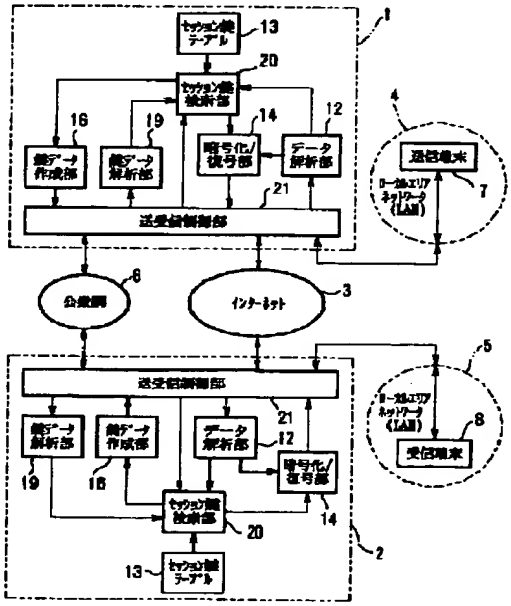
(72) Inventor: ONO SEIJI

(54) ENCRYPTION GATEWAY DEVICE

(57) Abstract:

PROBLEM TO BE SOLVED: To provide an encryption gateway device by which encryption communication with high security is realized without giving effect on the hardware and the application program of an existing terminal.

SOLUTION: Encryption gateway devices 1, 2 are placed on a border between local area networks 4, 5 and the internet 3 and encrypted data are transferred only through the internet 3 and key data are transferred through a route of a public network 6. Since the encrypted data and key data to decode the encryption are transferred through the routes physically different from each other, communication with high security is realized and since the encryption data are communicated without special revamping of a destination terminal, the cost increase to secure the confidentiality is minimized.



(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号

特開平11－68730

(43)公開日　平成11年(1999)３月９日

(51)Int.Cl.[6]		識別記号	FI		
Ｈ０４Ｌ	9/08		Ｈ０４Ｌ	9/00	６０１Ｂ
	9/10				６０１Ｅ
	12/46				６２１Ａ
	12/28			11/00	３１０Ｃ
	12/66			11/20	Ｂ

審査請求　有　　請求項の数３　ＯＬ　（全８頁）

(21)出願番号　特願平9－220478

(22)出願日　平成９年(1997)８月15日

(71)出願人　000232254
日本電気通信システム株式会社
東京都港区三田１丁目４番28号

(72)発明者　小野　誠司
東京都港区三田１丁目４番28号　日本電気通信システム株式会社内

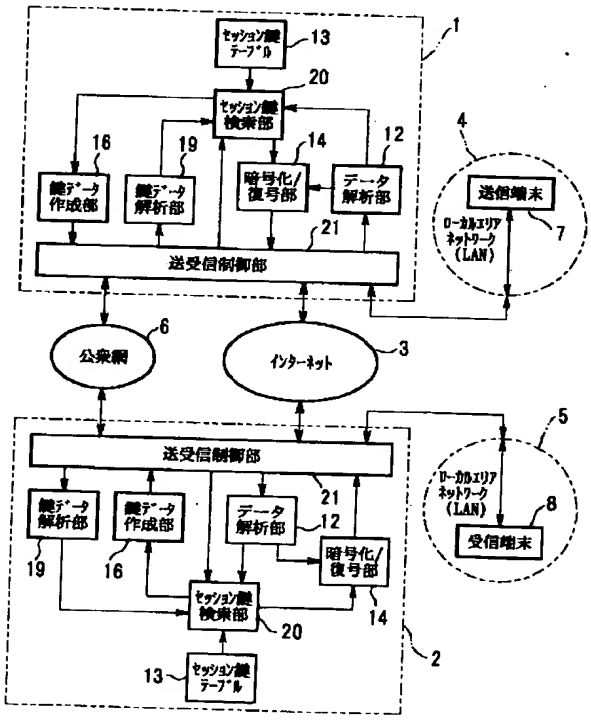
(74)代理人　弁理士　志賀　正武

(54)【発明の名称】　暗号ゲートウェイ装置

(57)【要約】

【課題】　既存の端末のハードウェア及びアプリケーションプログラムに影響を与えることなく機密性の高い暗号化通信を実現する暗号ゲートウェイ装置を提供する。

【解決手段】　ローカルエリアネットワーク４、５とインターネット３の境界に暗号ゲートウェイ装置１、２を置き、インターネット３を通る間だけ暗号化したデータにて転送を行い、鍵データは公衆網６のルートで転送する。これにより、暗号化データと、その暗号を解くための鍵データとが物理的に異なるルートで転送されるので、機密性の高い通信を実現でき、また送信先の端末に特別な改造をすることなく暗号化通信ができるので、機密性保持のためのコストの上昇を最小限に抑えることができる。



1

【特許請求の範囲】

【請求項１】　送信端末からの情報を受信し、その受信情報の暗号化／復合を行う暗号ゲートウェイ装置であって、

送信端末及び受信端末の識別情報と暗号化又は復合のためのセッション鍵の組を保持するセッション鍵テーブルと、

このセッション鍵テーブルから該当するセッション鍵を検索するセッション鍵検索手段と、

暗号化を行うための確認データ等を送受信するデータ送信手段及びデータ受信手段と、

暗号データや確認データ等を解析するデータ解析手段と、

受信した暗号化データ又は通常データを暗号化又は復合する暗号化／復合手段と、

暗号化を解く鍵データをダイヤルアップ等により別ルートにて受け渡しするための鍵データ送信手段及び鍵データ受信手段と、

受信した鍵データを解析する鍵データ解析手段と、

セッション鍵検索の結果で鍵データを作成する鍵データ作成手段と、

を備え、

ユーザからの暗号化指示により、暗号化データと鍵データを物理的に別ルートで転送することを特徴とする暗号ゲートウェイ装置。

【請求項２】　前記暗号化データをインターネットを使用して転送し、前記鍵データを公衆網を使用して転送することを特徴とする請求項１記載の暗号ゲートウェイ装置。

【請求項３】　前記暗号化データをインターネットを使用して転送し、前記鍵データを専用回線を使用して転送することを特徴とする請求項１記載の暗号ゲートウェイ装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、暗号ゲートウェイ装置に係り、特に広範囲に分散した事業所間をインターネットを介して暗号化通信を行う暗号ゲートウェイ装置に関する。

【０００２】

【従来の技術】図６は従来の暗号通信システムの構成を示すブロック図である。この図において、端末１３０と端末１４０との間で通信を行う場合、一方の端末１３０のアプリケーションプログラム１３２（以下、ＡＰと略す）が鍵配送センタ１６０より通信に使用するセッション鍵１６２を取得する。端末１３０のＡＰ１３２は、このセッション鍵を通信相手の端末１４０に送信することで２台の端末１３０、１４０で共通のセッション鍵を共有し、このセッション鍵を用いて通信文を暗号化及び復合して暗号通信を行う。

2

【０００３】図７は従来の暗号ゲートウェイ装置１８０の構成を示すブロック図である。この図において、暗号ゲートウェイ装置１８０は、暗号化／復合を行うための固定セッション鍵１８１と、受信情報を受信するための受信部１８２と、受信情報を解析して通信文を抽出する受信情報解析部１８３と、固定セッション鍵１８１を利用して通信文を暗号化／復合する暗号化／復合部１８４と、暗号化／復合された通信文を送信する送信部１８５とから成る。

【０００４】図８は図７に示す暗号ゲートウェイ装置１８０を利用した暗号通信システムの構成を示すブロック図である。この図において、端末２１-1、２１-2、…、２１-mから成るＡグループの端末に暗号ゲートウェイ装置１８０-1が外付けされ、また端末３１-1、３１-2、…、３１-nから成るＢグループの端末に暗号ゲートウェイ装置１８０-2が外付けされる。暗号ゲートウェイ装置１８０-1、１８０-2のセッション鍵は固定であるため、端末２１-1と３１-2の暗号通信と、端末２１-mと端末３１-2の暗号通信とは共通のセッション鍵で暗号化される。端末２１-1と端末３１-1との通信を行う場合には暗号ゲートウェイ装置１８０-1と１８０-2とを介さない伝送路を用いて通信を行う。

【０００５】

【発明が解決しようとする課題】ところで、上述した従来の暗号通信システムにあっては、以下に示す問題点があった。第１の問題点は、インターネットというオープンなネットワークに於いて、データの転送を行う場合、第３者にデータをモニタされる可能性が高く、重要なデータの転送を容易に行うことができない。その理由は、現状使われている暗号化方式である公開鍵暗号方式を使用したとき、アルゴリズムが公開されているため、暗号を解くことは困難であるが不可能ではないからである。

【０００６】第２の問題点は、秘密鍵暗号化方式を使用した場合、暗号化する際どの秘密鍵を使用してデータを転送するかの、事前了解が必要であるので、データを転送するまでに時間がかかってしまう。

【０００７】そこで本発明は、既存の端末のハードウェア及びアプリケーションプログラムに影響を与えることなく機密性の高い暗号化通信を実現する暗号ゲートウェイ装置を提供することを目的としている。

【０００８】

【課題を解決するための手段】この目的達成のため、本発明による暗号ゲートウェイ装置は、送信端末からの情報を受信し、その受信情報の暗号化／復合を行う暗号ゲートウェイ装置であって、送信端末及び受信端末の識別情報と暗号化又は復合のためのセッション鍵の組を保持するセッション鍵テーブルと、このセッション鍵テーブルから該当するセッション鍵を検索するセッション鍵検索手段と、暗号化を行うための確認データ等を送受信するデータ送信手段及びデータ受信手段と、暗号データや

確認データ等を解析するデータ解析手段と、受信した暗号化データ又は通常データを暗号化又は復合する暗号化／復合手段と、暗号化を解く鍵データをダイヤルアップ等により別ルートにて受け渡しするための鍵データ送信手段及び鍵データ受信手段と、受信した鍵データを解析する鍵データ解析手段と、セッション鍵検索の結果で鍵データを作成する鍵データ作成手段とを備え、ユーザからの暗号化指示により、暗号化データと鍵データを物理的に別ルートで転送することを特徴とする。

【０００９】この構成によれば、暗号化データと、その暗号を解くための鍵データとが物理的に異なるルートで転送されるので、機密性の高い通信を実現できる。また、送信先の端末に特別な改造をすることなく暗号化通信ができるので、機密性保持のためのコストの上昇を最小限に抑えることができる。

【００１０】

【発明の実施の形態】以下、本発明の実施の形態を、図面例と共に説明する。図１は本発明に係る暗号ゲートウェイ装置の実施の形態を用いた暗号通信システムの構成図、図２は本実施の形態の暗号ゲートウェイ装置の構成を示すブロック図である。

【００１１】図１において、暗号ゲートウェイ装置１、２はインターネット３とローカルエリアネットワーク４、５との間に設置されている。また、暗号ゲートウェイ装置４、５はダイヤルアップのために公衆網６とも接続される。暗号ゲートウェイ装置１、２は、送信側の端末（例えば端末７）から送信された情報を受信し、その受信情報を暗号化又は復合し、この結果得られた送信情報を受信側の端末（例えば端末８）へ送信して暗号通信を行うものであり、送信及び受信する情報と鍵に関する情報とが物理的に別ルートで伝達する構成になっている。

【００１２】暗号ゲートウェイ装置１、２の夫々は、図２に示すように、送信側の端末から送信されるデータを受信するデータ受信手段１１と、送信側の端末から受けた暗号化指示に対して暗号化指示と転送データを識別するデータ解析部１２と、暗号化及び復合のためのセッション鍵の組を保持するためセッション鍵テーブル１３と、選択された鍵を使用しデータの暗号化及び復合を行う暗号化／復合部１４と、暗号化及び復合されたデータを送信するデータ送信手段１５と、送信側の端末からの送信指示により選択された鍵を通信相手側の暗号化ゲートウェイ装置に送信するための鍵データを作成する鍵データ作成部１６と、作成された鍵データを送信する鍵データ送信手段１７と、鍵データを受信する鍵データ受信手段１８と、受信した鍵データを解析する鍵データ解析部１９と、受信した鍵データの解析結果及び送信する鍵の検索を行うセッション鍵検索部２０とを備えている。

【００１３】なお、上記データ受信手段１１、データ送信手段１５、鍵データ送信手段１７及び鍵データ受信手段１８は送受信制御部２１を構成する。暗号化ゲートウェイ装置４、５では暗号化／復合が自動的に行われるので、送信者は暗号化指示を行いデータを原文のまま送信し、受信者は受信したデータをそのまま利用できる。したがって、受信側では端末に暗号化通信による特別な用意をする必要はない。

【００１４】次に、上記構成による暗号ゲートウェイ装置１、２の動作について説明する。図３は暗号ゲートウェイ装置１、２の動作を示すフローチャートである。なお、この説明において、ローカルエリアネットワーク４の端末７が送信側で、ローカルエリアネットワーク５の端末８が受信側とする。

【００１５】暗号ゲートウェイ装置１がデータを受信したとき（ステップＳ２００）、受信ポートの確認を行い（ステップＳ２０１）、ＬＡＮポートである場合、送信側の端末７からのデータであることが判る。送信側の端末７からのデータは、暗号化指示データ若しくは通常データであるため、暗号化指示データであるか否かの判断（ステップＳ２０２）を行う。暗号化指示データであると判断した場合、送信先ネットワークの暗号ゲートウェイ装置２へ暗号化データを送信できるかを問い合わせる（ステップＳ２０３）。暗号化の問い合わせを行った後、相手からダイヤルアップ番号が取得できたか否かの判断（ステップＳ２０４）を行い、取得できた場合、問い合せＯＫであり、暗号化の準備を行う。これに対し、ダイヤルアップ番号の取得ができなかった場合は送信端末側に暗号化ＮＧの報告を行う（ステップＳ２０９）。

【００１６】ダイヤルアップ番号の取得ができると、セッション鍵の検索を行い（ステップＳ２０５）、この検索が完了すると、暗号鍵の作成を行い（ステップＳ２０６）、取得したダイヤルアップ番号へ暗号鍵を送信する（ステップＳ２０７）。また、それと同時に送信側の端末７からのデータを暗号化するため、暗号化／復合部１４へ暗号式の設定を行う（ステップＳ２０８）。

【００１７】送信側の端末７から受け取るデータが暗号化指示データでない場合、通常データであるため、そのデータが暗号化の必要なデータであるか否かの判断を行い（ステップＳ２１０）、暗号化が不必要な場合は原文のまま送信する（ステップＳ２１１）。暗号化が必要な場合はセッションの確認を行い（ステップＳ２１２）、さらに設定されている暗号化式にて暗号処理を行い（ステップＳ２１３）、インターネット３へ送信する（ステップＳ２１４）。

【００１８】一方、データ受信ポートがインターネットポートである場合、そのデータが暗号化問い合せデータであるか否かの判断を行う（ステップＳ２１５）。暗号問い合せデータである場合、ダイヤルアップ番号を問い合せをしてきた暗号化ゲートウェイに対して応答を行う（ステップＳ２１６）。インターネットポートから受信したデータは暗号化問い合せデータ、暗号化データ、通

常データの三つが考えられる（ステップＳ２１５、２１６）。

【００１９】インターネット３から受信したデータが暗号化問い合せデータでない場合、暗号化データまたは通常データが考えられる、通常データは、通常のゲートウェイとして原文のままＬＡＮポートへ出力する（ステップＳ２２０）。暗号化データを受信した場合はセッションの確認を行い（ステップＳ２１８）、さらに設定されている復合化式により復合処理を行い（ステップＳ２１９）、復合処理が完了した後にＬＡＮポートへ出力する（ステップＳ２２０）。受信したポートがダイヤルアップポートである場合、鍵データの解析を行い（ステップＳ２２１）、さらにセッション鍵の検索を行う（ステップＳ２２２）。そして、セッション鍵の検索後、暗号化／復合部１４にて復合処理（ステップＳ２２３）を行う。

【００２０】次に、図４は図１を詳細に示したものであり、この図を参照してローカルエリアネットワーク４の端末７からローカルエリアネットワーク５の端末８へインターネット３を使用して暗号化データを送る場合の動作について説明する。なお、説明の都合上区別し易いように、暗号ゲートウェイ装置１にはその各部の符号に”Ａ”を付加し、暗号ゲートウェイ装置２にはその各部の符号に”Ｂ”を付加する。

【００２１】送信側の端末７から暗号ゲートウェイ装置１の送受信制御部２１Ａに暗号指示データが送出される。送受信制御部２１Ａで受け取った暗号指示データはデータ解析部１２Ａにて解析が行われ、暗号指示データであるため、インターネット３を経由してローカルエリアネットワーク５側の暗号化ゲートウェイ装置２の送受信制御部２１Ｂへ暗号化問い合せデータを送信する。

【００２２】暗号ゲートウェイ装置２の送受信制御部２１Ｂは、問い合せの応答としてダイヤルアップ番号をインターネット３を通して暗号ゲートウェイ装置１の送受信制御部２１Ａへ送信する。暗号ゲートウェイ装置１の送受信制御部２１Ａはダイヤルアップ番号を受け取ると、セッション鍵検索部２０Ａにてセッション鍵テーブル１３Ａを参照し、セッション鍵の検索を行う。そして、セッション鍵が決定すると、鍵データ作成部１６Ａにて鍵データが作成され、送受信制御部２１Ａに鍵データが渡される。

【００２３】送受信制御部２１Ａで鍵データであると認識されると、送受信制御部２１Ａは先に通知されているダイヤルアップ番号へ公衆網６を使用し、鍵データを送信する。また、これと同時にセッション鍵検索部２０Ａは暗号化／復合部１４Ａに暗号式の設定を行う。送受信制御部２１Ａは受け取った鍵データを鍵データ解析部１６Ａにて解析し、セッション鍵検索部２０Ａがセッション鍵テーブル１３Ａを参照し、暗号化／復合部１４Ａへ復合式を設定する。

【００２４】送信側の端末７から暗号化対象のデータが暗号ゲートウェイ装置１の送受信制御部２１Ａへ送信されると、データ解析部１２Ａにてセッションの解析が行われ、暗号化の対象データと判断されると、暗号化／復合部１４Ａにて暗号化され、送受信制御部２１Ａからインターネット３を使用しデータ送信される。暗号データを受け取った暗号ゲートウェイ装置２では、データ解析部１２Ｂでセッションの解析が行われ、暗号化／復合部１４Ｂにて復合される。復合されたデータは送受信制御部２１Ｂから受信側の端末８へ送信され、受信側の端末８にて受け取られる。

【００２５】このように、この実施の形態では、ローカルエリアネットワーク４、５とインターネット３の境界に暗号ゲートウェイ装置１、２が置かれ、インターネット３を通る間だけ暗号化したデータにて転送を行い、鍵データは公衆網６のルートで転送する。したがって、暗号化データと、その暗号を解くための鍵データとが物理的に異なるルートで転送されるので、機密性の高い通信を実現でき、また送信先の端末に特別な改造をすることなく暗号化通信ができるので、機密性保持のためのコストの上昇を最小限に抑えることができる。なお、上記実施の形態では、鍵データを公衆網６を介して転送するようにしたが、図５に示すように専用の回線９を介して転送するようにしても良い。

【００２６】

【発明の効果】本発明によれば、鍵データを公衆網又は専用回線を使用し、暗号化データと同じルートで送信しない手順を踏むようにしているので、オフライン処理を必要とせず、秘密鍵暗号化方式を使用することができる。また、暗号ゲートウェイ装置で暗号化／復合処理を行うようにしたので、セキュリティに不安のあるインターネット上での機密性を保つことができる。また、送信先の端末に特別な改造をすることなく暗号化通信ができるので、機密性保持のためのコストの上昇を最小限に抑えることができる。

【図面の簡単な説明】

【図１】　本発明に係る暗号ゲートウェイ装置の実施の形態を用いた暗号通信システムの構成図である。

【図２】　実施の形態の暗号ゲートウェイ装置の構成を示すブロック図である。

【図３】　実施の形態の暗号ゲートウェイ装置の動作を示すフローチャートである。

【図４】　図１の暗号通信システムの詳細な構成を示すブロック図である。

【図５】　本発明に係る暗号ゲートウェイ装置の他の実施の形態を用いた暗号通信システムの構成図である。

【図６】　従来の暗号通信システム（その１）の構成を示すブロック図である。

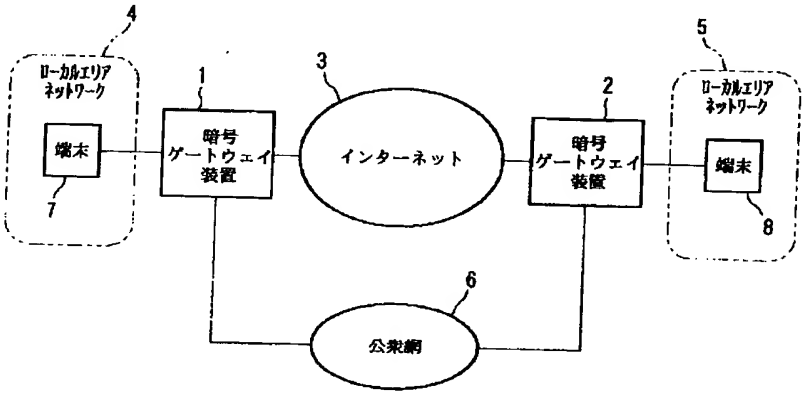
【図７】　従来の暗号ゲートウェイ装置の構成を示すブロック図である。

【図８】　図７の暗号ゲートウェイ装置を用いた暗号通信システム（その２）の構成を示すブロック図である。

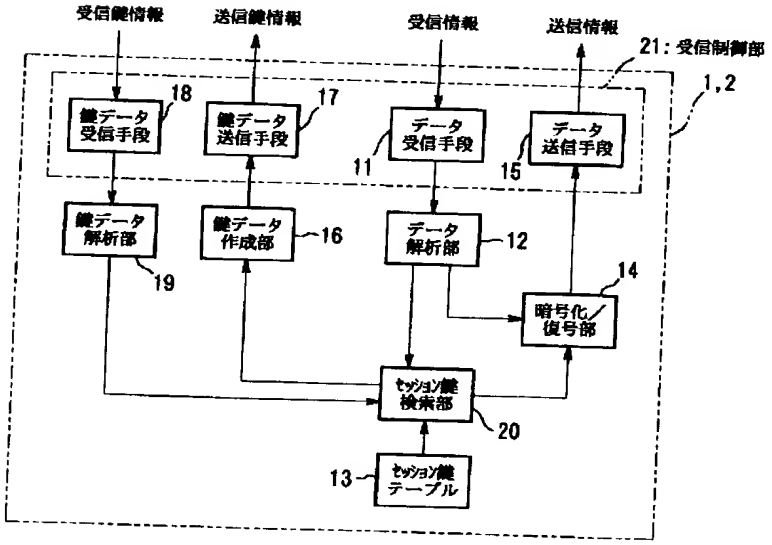
【符号の説明】

１、２　暗号ゲートウェイ装置
３　インターネット
４、５　ローカルエリアネットワーク
６　公衆網
７、８　端末
９　専用回線
１１　データ受信手段
＊１２　データ解析部
１３　セッション鍵テーブル
１４　暗号化／復合部
１５　データ送信手段
１６　鍵データ作成部
１７　鍵データ送信手段
１８　鍵データ受信手段
１９　鍵データ解析部
２０　セッション鍵検索部
＊10　２１　送受信制御部

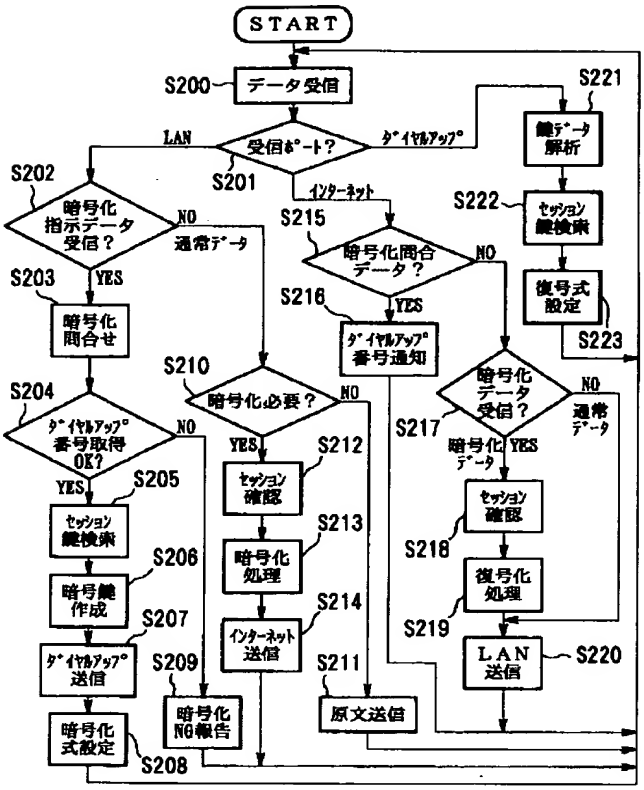
【図１】



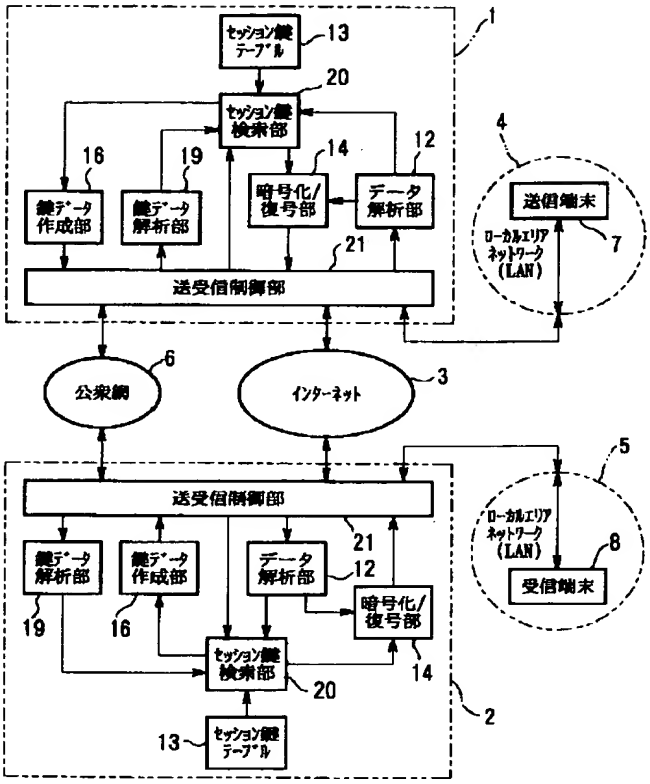
【図２】



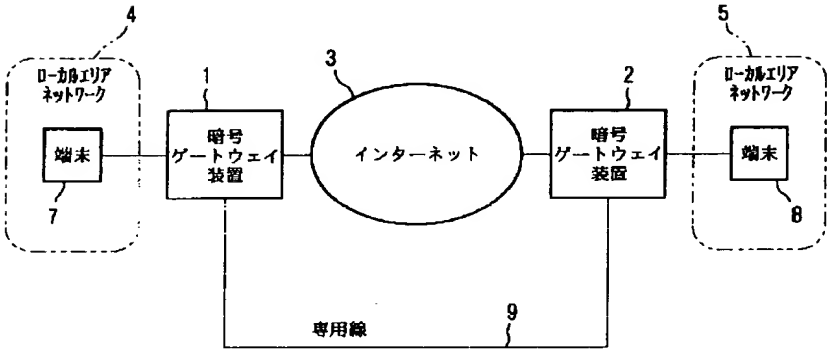
【図３】


START
S200
データ受信
S201
受信ポート？
LAN
ダイヤルアップ
インターネット
S202
暗号化指示データ受信？
NO
通常データ
YES
S203
暗号化問合せ
S204
ダイヤルアップ番号取得OK?
NO
YES
S205
セッション鍵検索
S206
暗号鍵作成
S207
ダイヤルアップ送信
S208
暗号化式設定
S209
暗号化NG報告
S210
暗号化必要？
NO
YES
S211
原文送信
S212
セッション確認
S213
暗号化処理
S214
インターネット送信
S215
暗号化問合データ？
NO
YES
S216
ダイヤルアップ番号通知
S217
暗号化データ受信？
NO
通常データ
暗号化データ
YES
S218
セッション確認
S219
復号化処理
S220
LAN送信
S221
鍵データ解析
S222
セッション鍵検索
S223
復号式設定

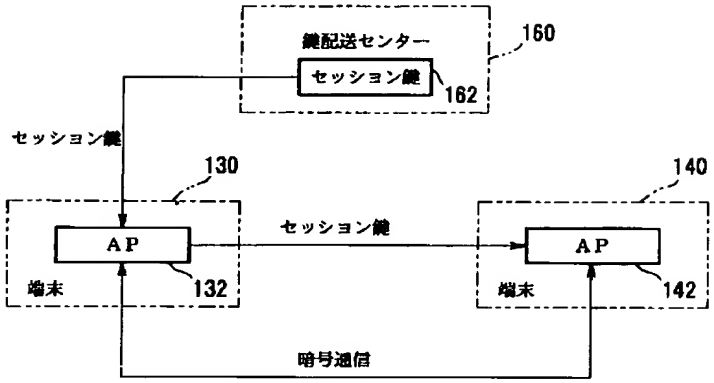
【図４】


1
セッション鍵テーブル
13
20
セッション鍵検索部
16
鍵データ作成部
19
鍵データ解析部
14
暗号化/復号部
12
データ解析部
21
送受信制御部
4
送信端末
ローカルエリアネットワーク(LAN)
7
公衆網
6
インターネット
3
5
送受信制御部
21
鍵データ解析部
19
鍵データ作成部
16
データ解析部
12
暗号化/復号部
14
セッション鍵検索部
20
13
セッション鍵テーブル
2
ローカルエリアネットワーク(LAN)
8
受信端末

【図５】

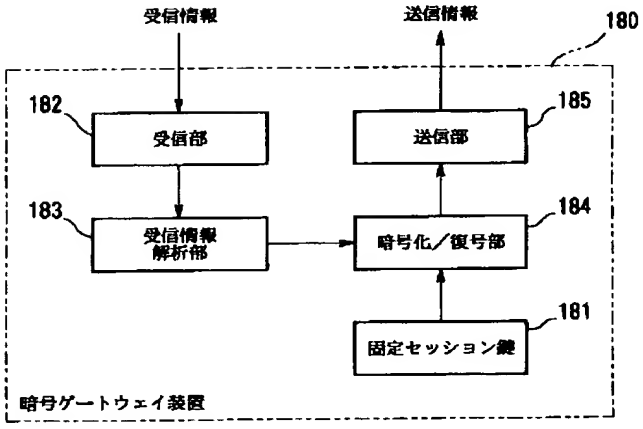

4
ローカルエリアネットワーク
端末
7
1
暗号ゲートウェイ装置
3
インターネット
2
暗号ゲートウェイ装置
5
ローカルエリアネットワーク
端末
8
専用線
9

【図６】



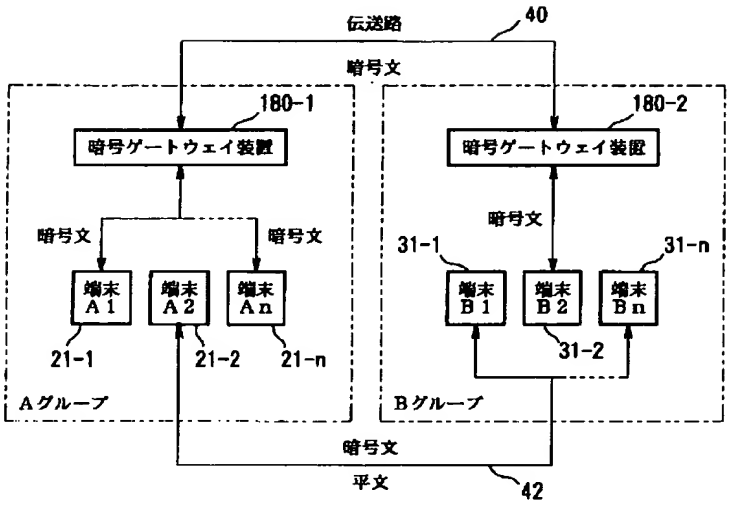
従来技術（１）

【図７】



従来技術（２）

【図８】


伝送路
40
暗号文
180-1
暗号ゲートウェイ装置
180-2
暗号ゲートウェイ装置
暗号文
暗号文
暗号文
31-1
31-n
端末 A1
端末 A2
端末 An
端末 B1
端末 B2
端末 Bn
21-1
21-2
21-n
31-2
Aグループ
Bグループ
暗号文
平文
42

従来技術（２）